Amendments to the Specification

Page 6, line 14

To describe the process of key usage control in more detail, refer now to the following discussion in conjunction with the accompanying Figure. A process for key usage control in accordance with a preferred embodiment of the present invention is illustrated in the flow diagram of Figure 3. In this process, first key pair material including tag information is created for a particular level, via step 302. Preferably, the creation of the key pair material occurs in a standard manner for the embedded security chip with the exception that now tag information is included with the key pair material. The key pair tag information combination is then loaded material onto the embedded security system, via step 304. When the key pair material is loaded onto the embedded security system, the predefined process of loading includes a check for the status of the tag by the embedded security chip internally, via step 306. If the tag indicates that the key is a binding-required key, the embedded security chip only allows cryptographic functions to be performed using this key if the system is bound, via step 308. If the tag indicates that the key is not designated as a binding required key, the embedded security chip allows all operations on the embedded security chip with that key regardless of binding, under the assumption that the user is verified by their password, via step 310. By way of example, a single bit could be used to indicate a set/reset status, where a set status indicates that the key is a binding-required key and a reset status indicates that the key is not a binding-required key.